AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for communicating cryptographic data through multiple network layers, comprising:

receiving the cryptographic data at a node;

dividing the cryptographic data into multiple pieces; and

simultaneously encapsulating different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields associated with different network layers of the protocol stack;

wherein the multiple fields ~~need to be~~are received simultaneously by a receiving node ~~to~~that reconstructs an identity associated with the cryptographic data; and

wherein the multiple fields ~~need to be~~are encapsulated simultaneously into the data packet to ensure that the data packet can be routed through a network to reach the receiving node.

2. (Original) The method of claim 1, wherein receiving the cryptographic data involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

3. (Original) The method of claim 2, wherein the input data includes a public key associated with the node.

4. (Original) The method of claim 2, wherein the input data includes a static identifier associated with the node.

5. (Original) The method of claim 2, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to "0".

6. (Original) The method of claim 5, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein

the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein

the host address is comprised of the IPv6 address.

7. (Original) The method of claim 2, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

8. (Original) The method of claim 2, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

9. (Original) The method of claim 2, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

10. (Original) The method of claim 2, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

11. (Currently Amended) An apparatus for communicating cryptographic data through multiple network layers, comprising:

a receiving mechanism configured to receive the cryptographic data at a node;

a dividing mechanism configured to divide the cryptographic data into multiple pieces; and

an encapsulation mechanism configured to simultaneously encapsulate different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields associated with different network layers of the protocol stack

wherein the multiple fields ~~need to be~~are received simultaneously by a receiving node ~~to~~that reconstructs an identity associated with the cryptographic data; and

wherein the multiple fields ~~need to be~~ are encapsulated simultaneously into the data packet to ensure that the data packet can be routed through a network to reach the receiving node.

12. (Original) The apparatus of claim 11, wherein the receiving mechanism is configured to perform at least one non-reversible function on a piece of input data to produce the cryptographic data.

13. (Original) The apparatus of claim 12, wherein the input data includes a public key associated with the node.

14. (Original) The apparatus of claim 12, wherein the input data includes a static identifier associated with the node.

15. (Original) The apparatus of claim 12, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to "0".

16. (Original) The apparatus of claim 15, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein
the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein
the host address is comprised of the IPv6 address.

17. (Original) The apparatus of claim 12, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

18. (Original) The apparatus of claim 12, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

19. (Original) The apparatus of claim 12, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

20. (Original) The apparatus of claim 12, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

21. (Currently Amended) A computer system for communicating cryptographic data through multiple network layers, comprising:

a central processing unit;

a semiconductor memory;

a receiving mechanism configured to receive the cryptographic data at a node;

a dividing mechanism configured to divide the cryptographic data into multiple pieces; and

an encapsulation mechanism configured to simultaneously encapsulate different pieces of the cryptographic data in fields associated with different network layers of a protocol stack in a data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is encapsulated within multiple fields associated with different network layers of the protocol stack;

wherein the multiple fields ~~need to be~~are received simultaneously by a receiving node ~~to~~ that reconstructs an identity associated with the cryptographic data; and

wherein the multiple fields ~~need to be~~are encapsulated simultaneously into the data packet to ensure that the data packet can be routed through a network to reach the receiving node.

22. (Original) The computer system of claim 21, wherein the receiving mechanism is configured to perform at least one non-reversible function on a piece of input data to produce the cryptographic data.

23. (Original) The computer system of claim 22, wherein the input data includes a public key associated with the node.

24. (Original) The computer system of claim 22, wherein the input data includes a static identifier associated with the node.

25. (Original) The computer system of claim 22, wherein an IPv6 address field of the data packet is comprised of a 64-bit prefix followed by the most-significant 64 bits of the output of the non-reversible function, and wherein a universal/local bit and an individual/group bit of the IPv6 address are both set to "0".

26. (Original) The computer system of claim 25, wherein a SIP Call-ID field of the data packet is comprised of a local-id and a host address, wherein

the local-id is comprised of the least-significant 128 bits of the output of the non-reversible function; and wherein

the host address is comprised of the IPv6 address.

27. (Original) The computer system of claim 22, wherein an SSH public-key fingerprint field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

28. (Original) The computer system of claim 22, wherein a MAC address field of the data packet is comprised of the least-significant 64 bits of the output of the non-reversible function.

29. (Original) The computer system of claim 22, wherein a JXTA Peer-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

30. (Original) The computer system of claim 22, wherein a JXTA Group-ID field of the data packet is comprised of the least-significant 128 bits of the output of the non-reversible function.

31. (Currently Amended) A method for verifying a data packet containing cryptographic data, comprising:

receiving the data packet;

extracting pieces of cryptographic data from fields associated with different network layers of a protocol stack within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is simultaneously encapsulated within multiple fields; and

verifying that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data;

wherein the multiple fields ~~need to be~~are received simultaneously to reconstruct an identity associated with the cryptographic data; and

wherein the multiple fields ~~need to be~~are simultaneously encapsulated into the data packet by a sending node to ensure that the data packet can be routed through a network to reach a receiving node.

32. (Original) The method of claim 31, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

33. (Previously Amended) An apparatus for verifying a data packet containing cryptographic data, comprising:

a receiving mechanism configured to receive the data packet;

an extracting mechanism configured to extract pieces of cryptographic data from fields associated with different network layers of a protocol stack within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is simultaneously encapsulated within multiple fields; and

a verification mechanism configured to verify that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data.

34. (Original) The apparatus of claim 33, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.

35. (Currently Amended) A computer system for verifying a data packet containing cryptographic data, comprising:

a central processing unit;

a semiconductor memory;

a receiving mechanism configured to receive the data packet;

an extracting mechanism configured to extract pieces of cryptographic data from fields associated with different network layers of a protocol stack within the data packet, wherein the cryptographic data is larger than a single field, and wherein the cryptographic data is simultaneously encapsulated within multiple fields; and

a verification mechanism configured to confirm that each piece of extracted cryptographic data matches with a corresponding portion of a piece of previously obtained cryptographic data;

wherein the multiple fields ~~need to be~~are received simultaneously to reconstruct an identity associated with the cryptographic data; and

wherein the multiple fields ~~need to be~~are simultaneously encapsulated into the data packet by a sending node to ensure that the data packet can be routed through a network to reach the receiving mechanism.

36. (Original) The computer system of claim 35, wherein the previously obtained cryptographic data is obtained through a process that involves performing at least one non-reversible function on a piece of input data to produce the cryptographic data.